IN THE CLAIMS:

Please amend claims 1, 5 – 8, 13, 14, 17, 21, 25, 29 – 31, and 35 as shown below. Please cancel claims 12, 16, 24, and 36 without prejudice or disclaimer. The following listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A portable storage device containing network identification information for a processing unit, the processing unit being connectable to a data communications network and including a device reader configured to read the portable storage device, the portable storage device comprising:

storage, the storage ~~configured to store~~ storing a network identity for the processing unit and at least one encryption key, wherein the network identity comprises a MAC address; and

an access controller, the access controller ~~being operable to control~~ controlling access to the storage by implementing key-key encryption, wherein the key-key encryption comprises asymmetric key encryption based on a public key and a corresponding private key.

2. (Original) The portable storage device of claim 1, comprising at least one secure storage portion accessible only under the control of the access controller.

3. (Original) The portable storage device of claim 2, wherein said at least one encryption key is held in said secure storage portion.

4. (Original) The portable storage device of claim 2, wherein at least one network security encryption key is held in said secure storage portion.

5. (Currently Amended) The portable storage device of claim 2, wherein a file is ~~configured~~ stored in said secure storage portion.

6. (Currently Amended) The portable storage device of claim 2, wherein one or more files containing information are ~~configured~~ stored in respective secure storage portions.

7. (Currently Amended) The portable storage device of claim 2, wherein the access controller ~~is operable to perform~~ performs ~~key-key~~ verification of a request encrypted by a request key supplied from the processing unit and, in response to the request key verifying correctly, ~~to return~~ returns to the processing unit an access key derived from said at least one encryption key to permit access to the secure storage portion.

8. (Currently Amended) The portable storage device of claim 7, wherein the access controller ~~is~~ subsequently ~~operable to respond~~ responds to a command from the processing unit that is encrypted using the access key to access the secure storage portion.

9. (Original) The portable storage device of claim 2, wherein the storage in the portable storage device comprises random access memory, the secure storage comprising a part of the random access memory.

10. (Original) The portable storage device of claim 1, wherein the access controller is a programmed microcontroller.

11. (Original) The portable storage device of claim 1, wherein the portable storage device is a smart card.

12. (Canceled)

13. (Currently Amended) A processing unit connectable to a data communications network, the processing unit comprising:

a device reader for a portable storage device, the portable storage device comprising storage and an access controller, the storage holding a network identity for

the processing unit and at least one encryption key, wherein the network identity comprises a MAC address, and the access controller controlling access to the storage by implementing key-key encryption, wherein the key-key encryption comprises asymmetric key encryption based on a public key and a corresponding private key, the processing unit ~~being operable to access~~ accessing a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller, and, in response to receipt of an access key from the access controller, ~~being operable to send~~ sending an encrypted command to access the content of the storage of the portable storage device.

14. (Currently Amended) The processing unit of claim 13, wherein, in response to the return of an access key, the processing unit ~~is operable to use~~ uses the access key to encrypt a command for access to a secure storage in the portable storage device.

15. (Original) The processing unit of claim 13, wherein the portable storage device is a smart card, the access controller is a microcontroller and the device reader is a smart card reader.

16. (Canceled)

17. (Currently Amended) The processing unit of claim 13, comprising a service processor, the service processor ~~being programmed to control~~ controlling reading of the portable storage device.

18. (Original) The processing unit of claim 17, wherein the service processor is a microcontroller.

19. (Original) The processing unit of claim 13, wherein the processing unit is a computer server.

20. (Original) The processing unit of claim 13, wherein the processing unit is a rack mountable computer server.

21. (Currently Amended) A computer-readable storage medium comprising a control program for a processing unit connectable to a data communications network, the processing unit comprising a device reader for a portable storage device that includes storage and an access controller, the storage holding a network identity for the processing unit and at least one encryption key, wherein the network identity comprises a MAC address, and the access controller controlling access to the storage by implementing key-key encryption, wherein the key-key encryption comprises asymmetric key encryption based on a public key and a corresponding private key, the control program being executable to implement:

accessing a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller; and

in response to receipt of an access key from the access controller, sending an encrypted command to access the content of the storage of the portable storage device.

22. (Previously Presented) The computer-readable storage medium of claim 21, wherein, in response to the return of an access key, the control program is executable to implement:

using the access key to encrypt a command for access to secure storage in the portable storage device.

23. (Previously Presented) The computer-readable storage medium of claim 21, wherein the portable storage device is a smart card, wherein the access controller is a microcontroller, and wherein the device reader is a smart card reader.

24. (Canceled)

25. (Currently Amended) The computer-readable storage medium of claim 21, wherein a service processor ~~is configured to control~~ controls reading of the portable storage device.

26. (Canceled)

27. (Previously Presented) The computer-readable storage medium of claim 21, wherein the processing unit comprises a service processor, the control program controlling operation of the service processor.

28. (Previously Presented) The computer-readable storage medium of claim 27, wherein the service processor is a microcontroller.

29. (Currently Amended) A microcontroller connectable to a data communications network, the microcontroller comprising:

a device reader for a portable storage device that includes storage and an access controller, the storage holding a network identity for the microcontroller and at least one encryption key, wherein the network identity comprises a MAC address, and the access controller controlling access to the storage by implementing key-key encryption, wherein the key-key encryption comprises asymmetric key encryption based on a public key and a corresponding private key; and

a control program ~~being operable to access~~ accessing a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller, and, in response to receipt of an access key from the access controller, ~~being operable to send~~ sending an encrypted command to access the content of the storage of the portable storage device.

30. (Currently Amended) A server computer comprising:

a device reader configured to read a portable storage device; and

a microcontroller, the microcontroller being operable as a service processor and connected to read the content of storage mounted in the portable storage device, the

microcontroller comprising a control program for a processing unit connectable to a data communications network, the processing unit having a device reader for the portable storage device that includes storage and an access controller, the storage holding a network identity for the processing unit and at least one encryption key, wherein the network identity comprises a MAC address, and the access controller controlling access to the storage by implementing key-key encryption, wherein the key-key encryption comprises asymmetric key encryption based on a public key and a corresponding private key, the control program ~~being operable to access~~ accessing a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller, and, in response to receipt of an access key from the access controller, ~~being operable to send~~ sending an encrypted command to access the content of the storage of the portable storage device.

31. (Currently Amended) A method for securing encryption keys for use in a processing unit connectable to a data communications network, the method comprising:

providing a portable storage device for a processing unit, wherein the processing unit is connectable to the data communications network, wherein the processing unit comprises a device reader configured to read the portable storage device, and wherein the portable storage device comprises storage and an access controller;

providing in the storage a network identity for the processing unit and at least one encryption key, wherein the network identity comprises a MAC address; and

implementing key-key encryption in the access controller for controlling access to the storage, wherein the key-key encryption comprises asymmetric key encryption based on a public key and a corresponding private key.

32. (Original) The method of claim 31, comprising defining at least part of the storage in the portable storage device as secure storage accessible only under the control of the access controller.

33. (Original) The method of claim 32, comprising storing said at least one encryption key in said secure storage.

34. (Original) The method of claim 32, comprising storing at least one network security encryption key in said secure storage.

35. (Currently Amended) The method of claim 31, comprising: the processing unit supplying a key-encrypted request to the access controller; the access controller providing ~~key-key~~ verification of the request key supplied from the processing unit; and in response to the key-encrypted request verifying correctly; returning to the processing unit an access key to permit access to the secure storage; the processing unit encrypting a command using the access key to access the secure storage; and the access controller responding to the first command to access the first storage.

36. (Canceled)